Self-Protected Quantum Algorithms Based on Quantum State Tomography

Lian-Ao Wu
Center for Quantum Information and Quantum Control
Chemical Physics Theory Group,
Department of Chemistry, University of Toronto,
80 St. George Street,
Toronto, Ontario, Canada M5S 3H6

Mark S. Byrd
Department of Physics and Department of Computer Science,
Southern Illinois University,
Carbondale, IL 62901

Only a few classes of quantum algorithms are known which provide a speed-up over classical algorithms. However, these and any new quantum algorithms provide important motivation for the development of quantum computers. In this article new quantum algorithms are given which are based on quantum state tomography. These include an algorithm for the calculation of several quantum mechanical expectation values and an algorithm for the determination of polynomial factors. These quantum algorithms are important in their own right. However, it is remarkable that these quantum algorithms are immune to a large class of errors. We describe these algorithms and provide conditions for immunity.

PACS numbers:

I. INTRODUCTION

There are only a few known quantum computing (QC) algorithms which provide a speed-up over their classical counterparts. The reasons for this are not completely clear [1, 2]. However, those algorithms and the associated techniques for solving problems efficiently are quite valuable [3, 4, 5]. For example, there are algorithms which belong to the same class as Shor's factoring algorithm [3] which enable the identification of a hidden abelian subgroup by using a quantum Fourier transform. There is another set of algorithms belonging to the same class as Grover's search algorithm [4] which can be applied to a wide class of problems where searching a solution set is the optimal known problem-solving strategy. Yet another class consists of algorithms for simulating quantum systems. Simulation algorithms can provide an exponential speed-up over any known classical algorithm for a variety of quantum systems [5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15] and are very promising for many applications in the physical sciences. These include atomic, molecular, solid state, and nuclear simulations and do not necessarily require a fully scalable quantum computing device [16].

To achieve the speed-ups promised by quantum computers, a reliable quantum information processing device is required. However, noise and imperfections still stand in our way. While the active strategies to prevent errors, such as quantum error correcting codes [17, 18, 19, 20] may, in principle, be universal as claimed, passive prevention methods have hardware resource advantages. For example, decoherence-free subspaces (DFS) and noiseless subsystems (NS) [21, 22, 23, 24] are based on the symmetry of the system-bath interaction, so do not require active detection and correction of errors. Another passive technique, holonomic quantum computation, is robust against stochastic errors in the control process [25, 26]. When conditions are appropriate, passive strategies can be applied during the design of quantum algorithms.

No matter which error prevention strategy is adopted however, it is widely believed that entanglement contributes to the errors in the system and is also the resource which is required to achieve the efficiencies promised by quantum computers. Here we take advantage of quantum entanglement in an obvious way in order to provide algorithms which solve some problems in polynomial time on a QC device. Our quantum algorithms, some of which are able to calculate quantities which are now clearly out of reach for classical computing devices, use quantum state tomography (QST) [27].

Our QST-based method complements the scattering circuit method [28, 29, 30, 31], the quantum phase estimation algorithms [32, 33, 34] it subsumes, and the adiabatic method we previously introduced for pairing Hamiltonians [15]. As our current method does, these other methods scale polynomially in the size of the input, and this is an exponential speedup over the best known classical algorithms for the same task. However, our algorithms are exceptional since they are immune to a large class of errors and therefore share some features with the passive error protection methods of DFS/NS. *Unlike this previous work, our emphasis is on the error resistance of the algorithms.*

Specifically, we first describe an algorithm for the determination of various types of observables that one may want to extract from a system which is being used as a quantum simulator. Second, we provide a method for the determination of the factors of a large polynomial using a quantum computing device. Our objectives are 1) to

show why these algorithms are robust against errors and 2) how these and other algorithms can take advantage of such inherent robustness.

II. ALGORITHM FOR OBTAINING THE EXPECTATION VALUES OF AN OBSERVABLE

Let us first consider the simulation of a quantum system of N subsystems (e.g., particles). It is well known that Hamiltonians H of the form $H = \sum_{k=1}^{L} H_k$, where L is a polynomial in N, and such that efficient quantum circuits exist for each term H_k (e.g., when all H_k have a tensor product structure or are simply sums of local terms), generate unitaries $U = \exp(iHt)$ which can be polynomially simulated [35]. Even random unitary matrices can be simulated polynomially [36]. Let us denote by $O(N^k)$ the simulation cost of such efficiently simulatable unitaries, where k is a fixed integer. This then yields an efficient algorithm for obtaining the quantum state $|\psi\rangle = U|000...0\rangle_N$.

The most general operator of non-identical d-level particles (qudits), up to two-body interactions, can be written as

$$\mathcal{O} = \sum_{ij\alpha\beta\gamma\delta} O_{\alpha\beta,\gamma\delta}(ij)|\alpha_i\beta_j\rangle\langle\gamma_i\delta_j|, \qquad (1)$$

where i, j label the N subsystems and $\alpha, \beta, \gamma, \delta \in \{0, 1, ..., d-1\}$ the states of the qudits, and $\{|\alpha_i\rangle\}$ is a basis for the Hilbert space of one qudit. For example, this could be a Hamiltonian or a unitary gate.

We are interested in the expectation value $\langle\mathcal{O}\rangle = \langle\psi|\mathcal{O}|\psi\rangle$ in a given quantum state $|\psi\rangle = U|\psi(0)\rangle$ where $|\psi(0)\rangle$ is an initial state. The existing classical algorithms for $\langle\mathcal{O}\rangle$ require the simulation of the unitary matrix U with $d^N \times d^N$ independent elements. Clearly, the classical simulation cost grows exponentially with the input. An efficient and general quantum method for obtaining $\langle\mathcal{O}\rangle$ when $\mathcal{O}$ is unitary is the "scattering circuit" [29]: one prepares an ancillary qubit in the state $(|0\rangle + |1\rangle)/\sqrt{2}$, interacts the main system with it using a controlled-U operation, then measures the Pauli operator σ^+ on the ancilla; this yields $\langle\mathcal{O}\rangle$ for qubits [28, 29, 30, 31] (we are unaware of a generalization of this method to qudits, though believe this is possible). The scattering circuit method includes quantum phase estimation algorithms [32, 33, 34] as special cases; its computational cost is $O(N^k)$. Here we introduce a different general method, based directly on QST [27]. Our method has a computational cost that is higher by a factor of $O(N^2)$ than the scattering circuit, but it does not require an ancilla and, more importantly, exhibits a remarkable inherent fault tolerance to decoherence errors.

To this end it is convenient to re-express $\langle\mathcal{O}\rangle$ in a form relevant to QST. The two-qudit reduced density matrix ρ^{ij} is given by $\rho^{ij} = \sum_m \langle m|\psi\rangle\langle\psi|m\rangle$, with m running over all the d^{N-2} orthonormal basis vectors, excluding qudits i and j. ρ^{ij} is $d^2 \times d^2$ dimensional, with elements $\rho^{ij}_{\gamma\delta,\alpha\beta} = \langle\gamma_i\delta_j|\hat{\rho}^{ij}|\alpha_i\beta_j\rangle = \sum_m \langle\gamma_i\delta_j m|\psi\rangle\langle\psi|m\alpha_i\beta_j\rangle = \sum_m \langle\psi|m\alpha_i\beta_j\rangle\langle\gamma_i\delta_j m|\psi\rangle = \langle\psi|\alpha_i\beta_j\rangle\langle\gamma_i\delta_j|\psi\rangle$, where we have used that $\langle\psi|m\alpha_i\beta_j\rangle$ are c-numbers and $\sum_m |m\rangle\langle m| = 1$. Using Eq. (1) we thus have

$$\langle\mathcal{O}\rangle = \sum_{ij\alpha\beta\gamma\delta} O_{\alpha\beta,\gamma\delta}(ij)\rho^{ij}_{\gamma\delta,\alpha\beta} = \sum_{ij} \mathrm{Tr}(O(ij)\rho^{ij}). \qquad (2)$$

This expression implies an efficient quantum algorithm for $\langle\mathcal{O}\rangle$, as follows: (0) Classically calculate the $d^2 \times d^2$ matrix elements $O_{\alpha\beta,\gamma\delta}(ij)$ for all $N(N-1)/2$ distinct pairs of qudits, in the fixed basis $\{|\alpha_i\rangle\}$. (i) Propagate $|\psi(0)\rangle$ to $|\psi\rangle$ using U, which can be done in $O(N^k)$ steps as noted above. (ii) Using QST find the $d^4 - 1$ real components of ρ^{ij} (for a given pair of qudits i, j). (iii) Repeat steps (i) and (ii) for all $N(N-1)/2$ distinct pairs of qudits. (iv) Repeat step (iii) M times, to obtain an estimate of $\langle\mathcal{O}\rangle$ with a precision (standard deviation) that scales as $1/\sqrt{M}$(central limit theorem). (iv) Classically evaluate $\sum_{ij} \mathrm{Tr}(O(ij)\rho^{ij})$. The total simulation cost is $O(d^4 M N^{k+2})$. However, we may note that this might be improved using more recent QST methods [37].

Note that this method can be generalized to the case of n-local observables with many-body correlations. Specifically, any operator on N qudits can be expressed as a linear combination of terms, each of which is a tensor product of N generalized Pauli matrices (e.g., the "very nice error operator basis" [38, 39]), where we include the $d \times d$ identity as a generalized Pauli matrix. If each of these tensor products contains at most n generalized Pauli matrices not equal to the identity then the operator is said to be n-local. In the case of a n-local operator the obvious generalization of Eq. (2) is $\langle\mathcal{O}\rangle = \sum_{i_1 i_2 ... i_n} \mathrm{Tr}(O(i_1 i_2 ... i_n)\rho^{i_1 i_2 ... i_n})$, where $\rho^{i_1 i_2 ... i_n}$ is the $d^n \times d^n$ dimensional reduced density matrix of particles $i_1 i_2 ... i_n$. Its $d^{2n} - 1$ real components can be obtained via QST, again using a fixed number M of copies of $|\psi(0)\rangle$. This must be done for all $\binom{N}{n}$ n-tuples of particles. Therefore the total computational cost of our algorithm for the expectation value in the case of n-local observables is $O(d^{2n} M N^{k+n})$. The measurement error $\epsilon = \langle(\mathcal{O} - \mathcal{O}_{\mathrm{est}})^2\rangle_{\mathrm{ave}}$ (where $\mathcal{O}_{\mathrm{est}}$ is the estimator employed and averaging is with respect to the M repetitions) satisfies the generalized uncertainty relation (derived from the Cramer-Rao bound) [40]: $\epsilon\Delta H \geq 1/(2\sqrt{M})$, where $\Delta H = (\langle H\rangle^2 - \langle H^2\rangle)^{1/2}$ is the variance of H on the input state $|\psi(0)\rangle$. This bound is independent of n but depends implicitly on d through ΔH. It is important to note that if $|\psi(0)\rangle$ is itself an entangled state of P identical copies then the measurement error can be reduced by a factor of P (the Heisenberg limit); the details and a general proof of optimality of this bound, as well as its achievability, are discussed in [41].

An important special case is when $|\psi\rangle$ is an eigenstate of a Hamiltonian. The energy spectrum may then be found by preparing a (complete) set of eigenstates

$|\psi_n\rangle$ and measuring the set of expectation values $\langle\mathcal{O}\rangle_n = \langle\psi_n|H|\psi_n\rangle = E_n$. Let us comment on precision issues in this context. Our QST-based method complements the scattering circuit method [28, 29, 30, 31] and the quantum phase estimation algorithms [32, 33, 34] it subsumes, and the adiabatic method we previously introduced for pairing Hamiltonians [15]. As in our current method, these other methods scale polynomially in N, and this is commonly considered an exponential speedup over the currently known best classical algorithms for the same task. However, for error ϵ (defined above) the number of digits of precision l in the result is $l \tilde{} \log(1/\epsilon)$, and both the scattering circuit and the adiabatic methods require poly$(1/\epsilon)$ elementary steps to obtain this precision, due to the use of the (quantum) Fourier transform at the measurement [42]. In contrast, an efficient algorithm would only require poly$(\log(1/\epsilon))$ number of steps. As observed by Brown et al. [42], while this has no impact for fixed precision, the $1/\epsilon$ scaling does imply an exponential scaling with the number of digits of precision. The origin of the $l \tilde{} \log(1/\epsilon)$ scaling is illucidated by Giovannetti et al. [41], who show that this scaling cannot be improved even using entanglement. Namely, they show that entangled measurements do not help, and the use of P entangled input probes gives at most the Heisenberg limit $\epsilon \tilde{} 1/P$, and on the other hand $l \tilde{} \log P$. Thus $l \tilde{} \log(1/\epsilon)$. While our QST based method does not employ a Fourier transform at the measurement, the general arguments used in [41] apply to QST as well, so that our present algorithm does not improve on the precision issue. As discussed in [42], the origin of the poly$(1/\epsilon)$ number of steps is in the use of the Trotter formula for the simulation of U. Use of the Solovay-Kitaev theorem [which improves the Trotter poly$(1/\epsilon)$ scaling to $O(\log^2(1/\epsilon))$ scaling] does not help when a fault tolerant implementation is considered, since the latter once again leads to the poly$(1/\epsilon)$ scaling [42]. However, it is important to note that these general bounds do not preclude specific Hamiltonians from being efficiently simulatable in terms of precision requirements; indeed the exponential precision slow-down is avoided in Shor's algorithm due to the manner in which modular exponentiation is carried out [3]. Another observation is that in some cases it is possible to prepare the final state $|\psi\rangle$ by means other than quantum simulation, e.g., via cooling to the ground state, or via adiabatic evolution. There are certainly examples where then reaching $|\psi\rangle$ from $|\psi(0)\rangle$ requires poly$(\log(1/\epsilon))$ steps.

III. ALGORITHM FOR OBTAINING THE EXPECTATION VALUES OF AN OBSERVABLE OF A FERMIONIC SYSTEM

It follows from the Jordan-Wigner transformation [43] that there is one-to-one correspondence between fermions characterized by the fermionic creation and annihilation operations $c_j^\dagger$ and c_j, where j denotes a fermionic mode, and qubits: $c_j^\dagger \Leftrightarrow (-1)^{j-1}\left(\bigotimes_{l=1}^{j-1}\sigma_l^z\right)\sigma_j^+$ [$\sigma^\pm = (\sigma^x \pm i\sigma^y)/2$ and $\sigma^{x,y,z}$ are the Pauli matrices]. Therefore, the above algorithm can be applied to a fermionic system. However, a one-body or two-body interactions of fermions usually corresponds to a many-body interaction of qubits, for instance $c_i^\dagger c_j \Leftrightarrow (-1)^{i+j}\left(\bigotimes_{l=i}^{j-1}\sigma_l^z\right)\sigma_i^z ... \sigma_{j-1}^z \sigma_i^+ \sigma_j^-$ where $j > i$. Even so, it is clear that obtaining the expectation value of an observable with many-body correlation still requires only polynomial time. For example, measuring an observable such as $\sigma_i^x \sigma_j^x \sigma_{i+1}^z ... \sigma_{j-1}^z$ can be accomplished efficiently, as long as the distance between i and j is finite and independent of N. In some cases *partial* QST suffices to obtain a desired expectation value. For example, consider the one-body Fermi operator $h = \sum \epsilon_i n_i$ ($n_i = c_i^\dagger c_i$), where we assume the ϵ_i are known. Then

$$
\begin{aligned}
{}_f\langle\psi|\, h\, |\psi\rangle_f &= \sum \epsilon_i\, {}_f\langle\psi|\, n_i\, |\psi\rangle_f \\
&\Leftrightarrow \sum \epsilon_i \langle\psi| \frac{1-\sigma_i^z}{2} |\psi\rangle = \sum \epsilon_i |c_{\alpha_1 ... 0_i ... \alpha_N}|^2 \\
&= \sum \epsilon_i \rho_{11}^i, \qquad (3)
\end{aligned}
$$

where $|\psi\rangle = \sum_{i=1}^N \sum_{\alpha_i=0}^1 c_\alpha |\alpha\rangle$ ($\alpha = \{\alpha_1, ..., \alpha_N\}$) is an arbitrary pure state of N qubits and $\rho_{11}^i = (\mathrm{Tr}_{j\neq i} |\psi\rangle\langle\psi|)_{11}$, $j = 1...N$. $\Leftrightarrow$ means that there is a one-to-one correspondence between $|\psi\rangle_f$ expressed by Fermi creation operators on the vacuum state and $|\psi\rangle$ expressed by the superposition of computational bases [44].

IV. INHERENT ROBUSTNESS

The accuracy of a usual quantum algorithm requires that the final wave function $|\psi_0\rangle$ or density matrix be $\rho_I = |\psi_0\rangle\langle\psi_0|$. In reality, due to errors, the actual density matrix will be given by $\rho_A = \sum_{k=0}^{2^N} p_k |\psi_k\rangle\langle\psi_k|$ which is different from the ideal one ρ_I. However as long as the following relations are satisfied;

$$\rho^i = \mathrm{Tr}_i \rho_I = \mathrm{Tr}_i \rho_A \quad \text{or,} \quad \rho^{ij} = \mathrm{Tr}_{ij} \rho_I = \mathrm{Tr}_{ij} \rho_A \qquad (4)$$

our algorithms will give the same results, where the subscripts i and j means trace over all degrees of freedom excluding i and j. There are only $3N$ or $15N^2$ constraints respectively. This implies that our algorithms are much more fault-tolerant than a generic one. The reason that the algorithms are more robust is that there are 2^N independent coefficients in ρ_A. However, we only require that the above relation holds independent of the other various parameters in the system.

As a motivational example, suppose an expected final state is $|\psi_0\rangle = a|00\rangle + b|11\rangle$, but due to dephasing errors, we actually get

$$\rho_A = |a|^2 |00\rangle\langle 00| + |b|^2 |11\rangle\langle 11| + C|00\rangle\langle 11| + C^* |11\rangle\langle 00|$$

where C is an arbitrary number and is zero when complete phase damping occurs. No matter what value of C,

$$\rho^1 = \rho^2 = \begin{bmatrix} |a|^2 & 0 \\ 0 & |b|^2 \end{bmatrix}.$$

Therefore, dephasing does not affect the validity of our algorithm in this case. The algorithms are, to some extent, self-protected.

To provide some general conditions under which our algorithms are robust, let us start with some definitions. Let

$$\rho = \rho_A \otimes \rho_B \otimes \rho_E, \tag{5}$$

where ρ_A is the subsystem we wish to study, ρ_B is the rest of our system, and ρ_E is the density operator for the environment. We can assume that each of these is a pure state and the whole system plus environment is pure and initially completely separable. Now, let $U \otimes I_E$ be the ideal unitary operation for our simulation algorithm and

$$\rho_I = U \otimes I_E \rho U^\dagger \otimes I_E. \tag{6}$$

Let V be the non-ideal operation. We can write the condition for the algorithm to give the same result for the expectation value of an operator $\mathcal{O}$ as $\mathrm{Tr}(\mathcal{O}\rho') = \mathrm{Tr}(\mathcal{O}W\rho' W^\dagger)$, where $W = V(U^\dagger \otimes I_E)$. Let the basis for the algebra of operators be traceless and Hermitian and represented by $\lambda_\alpha^{(i)}$, $i = 1, 2, 3$, for subsystems A, B, E respectively with $\alpha \in \{1, ..., d^2 - 1\}$. Then we may write the density operator for the ABE system as

$$\begin{aligned} \rho_{ABE} &= I_{ABE} + \sum_i a_i \lambda_i^{(1)} + I_A \otimes \sum_j b_j \lambda_j^{(2)} \otimes I_E \\ &\quad + I_{AB} \otimes \sum_k c_k \lambda_k^{(3)}. \end{aligned} \tag{7}$$

If $\mathcal{O} = \vec{n} \cdot \vec{\lambda}^{(1)}$ (or $\mathcal{O} = \vec{n} \cdot \vec{\lambda}^{(1)} \otimes I_E$), then $\mathcal{O}$ acts as a projector onto the subspace A and the expectation value of $\mathcal{O}$ is

$$\langle \mathcal{O} \rangle = \mathrm{Tr}(\mathcal{O}W\rho' W) = \mathrm{Tr}(\vec{n} \cdot \vec{\lambda}^{(1)} W \rho' W). \tag{8}$$

So if $W\rho' W^\dagger$ has the form ρ_{ABE}, then $\langle \mathcal{O} \rangle = \vec{n} \cdot \vec{a}$, where $\vec{a} = \{a_1, a_2, \dots\}$. Likewise, if

$$\rho' = I_{AB} + \sum_i a_i^I \lambda_i^{(1)} \otimes I_B + I_A \otimes \sum_j b_j^I \lambda_j^{(2)}, \tag{9}$$

then $\mathrm{Tr}(\mathcal{O}\rho') = \vec{n} \cdot \vec{a}^I$. Therefore, for these to be equal, we require that $\vec{n} \cdot \vec{a} = \vec{n} \cdot \vec{a}^I$. If we write $\vec{n} \cdot \vec{a}^I = |\vec{n}||\vec{a}^I| \cos\theta^I$, and $\vec{n} \cdot \vec{a} = |\vec{n}||\vec{a}| \cos\theta$, then we need $|\vec{a}^I| \cos\theta^I = |\vec{a}| \cos\theta$. For a two-state subsystem A, this leaves one degree of freedom, the little group of the vector $\vec{a}$. This is stated in terms of the coherence vector for a general expectation value for a d-state system.

We may also show that the robustness can be expressed in terms of the expectation value of the operator $\mathcal{O}$ and completely positive (CP) maps. Let us choose an initial density matrix ρ which will be acted upon by a CP map corresponding to the operator-sum decomposition with operators A_i. We then want to find:

$$\langle \mathcal{O} \rangle_1 = \mathrm{Tr}(\mathcal{O} \sum_i A_i \rho A_i^\dagger). \tag{10}$$

Note that this can be written as

$$\langle \mathcal{O} \rangle_1 = \mathrm{Tr}(\sum_i A_i^\dagger \mathcal{O} A_i \rho) \tag{11}$$

so that the condition for the same result to be obtained from a different set of operators B_i is

$$\begin{aligned} 0 &= \langle \mathcal{O} \rangle_1 - \langle \mathcal{O} \rangle_2 \\ &= \mathrm{Tr}\left(\sum_i A_i^\dagger \mathcal{O} A_i \rho \right) - \mathrm{Tr}\left(\sum_j B_j^\dagger \mathcal{O} B_j \rho \right) \\ &= \mathrm{Tr}\left[\left(\sum_i A_i^\dagger \mathcal{O} A_i - \sum_j B_j^\dagger \mathcal{O} B_j \right) \rho \right]. \end{aligned} \tag{12}$$

Therefore, we may also say that the expectation value is invariant under transformations which are comprised of the little group of $\mathcal{O}$. This is true for both the unitary description above, as well as the operator-sum decomposition.

Let us simplify to the case of a qubit. Letting $\mathcal{O}$ be traceless and Hermitian and $B_j = \beta_j I + \vec{b}_j \cdot \vec{\sigma}$ and $A_i = \alpha_i I + \vec{a}_i \cdot \vec{\sigma}$ we may obtain the relation

$$\begin{aligned} \sum_i A_i^\dagger \mathcal{O} A_i &= \sum_i (iI(\vec{a}_i \times \vec{a}_i^*) \cdot \vec{n} \\ &\quad + (|\alpha_i|^2 - \vec{a} \cdot \vec{a}^*) n_t \sigma_t \\ &\quad + [\alpha_i (\vec{a}_i^* \times \vec{n})_t - \alpha_i^* (\vec{a}_i \times \vec{n})_t] \sigma_t \\ &\quad + [(\vec{a}_i^* \cdot \vec{n}) a_{it} + (\vec{a}_i \cdot \vec{n}) a_{it}^*] \sigma_t), \end{aligned} \tag{13}$$

where the sum over t is implied. Simplifying further by letting $\mathcal{O} = \sigma_3$ and $\rho = (1/2)(I + \sigma_3)$, we can write the condition as

$$\begin{aligned} &\sum_k [i(\vec{a}_k \times \vec{a}_k^*)_3 + (|\alpha_k|^2 - |a_{k1}|^2 - |a_{k2}|^2 + |a_{k3}|^2)] \\ &- \sum_j [i(\vec{b}_j \times \vec{b}_j^*)_3 - (|\beta_j|^2 - |b_{j1}|^2 - |b_{j2}|^2 + |b_{j3}|^2)] = 0. \end{aligned}$$

Note that $\sum_i A_i^\dagger A_i = I$, implies $\sum_i (|\alpha_i|^2 + \vec{a}_i \cdot \vec{a}_i^*) = 1$, and $\sum_i [\alpha_i a_{it}^* + \alpha_i^* a_{it} + i(\vec{a}_i \times \vec{a}_i^*)_t] = 0$. So the result can be expressed in terms of two equations

$$\begin{aligned} &\sum_k [i(\vec{a}_k \times \vec{a}_k^*)_3 - 2(|a_{k1}|^2 + |a_{k2}|^2)] \\ &- \sum_j [i(\vec{b}_j \times \vec{b}_j^*)_3 + 2(|b_{j1}|^2 + |b_{j2}|^2)] = 0. \end{aligned}$$

and

$$\sum_k [|\alpha_k|^2 + |a_{k3}|^2 + \alpha_k a_{k3}^* + \alpha_k^* a_{k3}]$$
$$- \sum_j [|\beta_j|^2 + |b_{j3}|^2 + \beta_j a_{j3}^* + \beta_j^* b_{j3}] = 0.$$

To summarize, *our simulation algorithms, based on quantum state tomography and the expectation value of an operator, are immune to errors which act as the little group of transformations of the initial density operator or the operator for which we seek the expectation value.*

V. ALGORITHM FOR FACTORING A POLYNOMIAL

We now present one more algorithm which can be implemented via state tomography and which is robust against the aforementioned class of errors. Consider variables x_i, y_i , where $i = 1, 2, ..., N$, and a class of homogeneous functions spanned by the set of products of x_i, y_i. For instance when $N = 2$, the set is x_1x_2, x_1y_2, y_1x_2 and y_1y_2. There is a one-to-one correspondence between this set and the computational basis for two qubits. The linear combination of the set defines a class of homogeneous functions. For instance, consider the two functions $x_1x_2 + y_1y_2$ and $x_1y_2 + y_1y_2$. The former cannot be factored, while the latter can be factored into the form $(x_1 + y_1) \times y_2$. In some circumstances, it may be easy to tell whether or not this can be factored, if we know the concrete form of the homogeneous function. However, if a homogeneous function contains many terms, in general it will become difficult. Consider such a function derived from a matrix U acting on a basis set such as $x_1x_2x_3...x_N$

$$f_N(x_i, y_i) = Ux_1x_2x_3...x_N \tag{14}$$

where U is a $2^N \times 2^N$ matrix. To represent the function, a classical computer needs to handle $2 \times 2^N \times 2^N$ independent numbers in $2^N \times 2^N$ complex matrix elements of U in order to simulate it. We may assume U is unitary so that it preserves the norm of the function. However, this still requires a classical simulation of $2^N \times 2^N$ independent numbers in the matrix U . When $N = 300$, approximately 10^{180} independent numbers must be handled.

Given a unitary matrix U which could be a random unitary matrix, or the quantum state $|f\rangle = U|000...0\rangle_N$, which can be simulated polynomially, say N^k, [36] where k is a fixed number, we will determine the presence of a factor $ax_i + by_i$. We first obtain the reduced density matrix of the ith qubit $\rho^i = (1/2)(I + \vec{n}^i \cdot \vec{\sigma}^i)$ by using quantum state tomography, which requires need a fixed number, M, copies of $|f\rangle$, as discussed above. Then, we calculate the von Neumann entropy of ρ^i. If the entropy is zero, the ith qubit is separable from the others, meaning that there is a factor $ax_i + by_i$ in $f_N(x_i, y_i)$ where $a = \sqrt{1 + n_z^i}$ and $b = (n_x^i + in_y^i)/\sqrt{1 + n_z^i}$ given by the matrix elements of ρ^i. Otherwise, there is no such factor. The total number of steps in the quantum procedure is MN^k. The same procedure can be used to find higher order factors. For example, a factor $ax_ix_j + bx_iy_j + cy_ix_j + dy_iy_j$ can be found by measuring the reduced density matrix ρ^{ij} for the ith and jth qubits.

Furthermore, the generalization to many-qudit systems, (each subsystem has an arbitrary dimension), and thus multivariate polynomials can be accomplished by using the generalized coherence vector, or generalized Bloch vector [45, 46, 47]. Let $\lambda_i^r \otimes \mu_j^s$ be a Hermitian basis for a system of coupled qudits, with arbitrary dimensions for all components. Let λ_i^r form a basis for the ith subsystem with $\mathrm{Tr}(\lambda_i^r \lambda_i^t) = 2\delta_{rt}$ and μ_j^s a basis for the rest of the system. Then, given the state $U|000...0\rangle$ for the whole system, the corresponding reduced density matrix for the ith subsystem has $\rho = (1/d)(\mathbb{1} + \vec{m} \cdot \vec{\lambda})$. The conditions for the system to be factorisable with respect to the ith subsystem is that $\vec{m} \cdot \vec{m} = N(N-1)/2$ and $d_i^{rst} m_r m_s N(N-1)/(2N-4) = m_t$, with $d_i^{rst} = (N/4)\mathrm{Tr}(\{\lambda_i^r, \lambda_i^s\}\lambda_i^t)$. As usual, $\{\cdot, \cdot\}$ denotes the anti-commutator. These conditions indicate that the qudit is in a pure state and thus has zero entropy. Using the Hermitian basis for the operators in this protocol provides an explicit measurement basis for the identification of the reduced density matrices.

VI. CONCLUSIONS

In this paper, we introduced quantum algorithms based on quantum state tomography. The simulation algorithms are clearly polynomial while the best known classical counterparts of the simulation algorithms are exponential. We suspect that the polynomial factoring algorithm is also more efficient although we have not proved this generally. Certainly in the case that the unitary U must be simulated, we achieve an exponential speed-up. We emphasize that the algorithms are, to a large degree, self-protected against a large class of errors. This work brings together two important aspects in quantum information science, algorithms and passive correction. We expect that the family of quantum algorithms which are error-avoiding algorithms should receive much more attention in future studies of quantum algorithms.

[1] P.W. Shor, J. ACM **50**, 87 (2003).

[2] P. Shor, Qu. Inf. Proc. **3** (2004).

[3] P.W. Shor, SIAM J. on Comp. **26**, 1484 (1997).

[4] L.K. Grover, in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (ACM, New York, NY, 1996), p. 212.

[5] R.P. Feynman, Intl. J. Theor. Phys. **21**, 467 (1982).

[6] S. Lloyd, Science **273**, 1073 (1996).

[7] D.A. Meyer, Phys. Rev. E **55**, 5261 (1997).

[8] B.M. Boghosian and W. Taylor, Phys. Rev. E **57**, 54 (1998).

[9] C. Zalka, Proc. Roy. Soc. London Ser. A **454**, 313 (1998).

[10] D.S. Abrams and S. Lloyd, Phys. Rev. Lett. **79**, 2586 (1997).

[11] B.M. Terhal, Phys. Lett. A **271**, 319 (2000).

[12] M.H. Freedman,A. Kitaev and Z. Wang, Commun. Math. Phys. **227**, 587 (2002).

[13] D.A. Lidar and H. Wang, Phys. Rev. E **59**, 2429 (1998), eprint quant-ph/9807009.

[14] G. Ortiz, J. E. Gubernatis, E. Knill and R. Laflamme, Phys. Rev. A **64**, 022319 (2001).

[15] L.-A. Wu, M.S. Byrd and D.A. Lidar, Phys. Rev. Lett. **89**, 057904 (2002).

[16] E. Jane, G. Vidal, W. Dür, P. Zoller, J.I. Cirac, Qu. Inf. & Comp. **3** (2003).

[17] P.W. Shor, Phys. Rev. A **52**, 2493 (1995).

[18] A. Steane, Rep. Prog. Phys. **61**, 117 (1998).

[19] A.R. Calderbank and P.W. Shor, Phys. Rev. A **54**, 1098 (1996).

[20] D. Gottesman, Ph.D. thesis, California Institute of Technology, Pasadena, CA (1997), eprint quant-ph/9705052.

[21] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).

[22] L.-M Duan and G.-C. Guo, Phys. Rev. A **57**, 737 (1998).

[23] D.A. Lidar, I.L. Chuang and K.B. Whaley, Phys. Rev. Lett. **81**, 2594 (1998).

[24] E. Knill, R. Laflamme and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).

[25] P. Zanardi and M. Rasetti, Phys. Lett. A **264**, 94 (1999).

[26] J. Pachos, P. Zanardi and M. Rasetti, Phys. Rev. A **61**, 010305(R) (1999).

[27] K. Vogel and H. Risken, Phys. Rev. A **40**, 2847 (1989).

[28] R. Somma, G. Ortiz, J. E. Gubernatis, E. Knill, and R. Laflamme, Phys. Rev. A **65**, 042323 (2002).

[29] J.P. Paz, A. Roncaglia, Phys. Rev. A **68**, 052316 (2003).

[30] C.M. Alves, P. Horodecki, D.K.L. Oi, L. C. Kwek and A.K. Ekert, Phys. Rev. A **68**, 032306 (2003).

[31] G.M. D'Ariano, C. Macchiavello, P. Perinotti, Phys. Rev. A **72**, 042327 (2005).

[32] A. Kitaev (1995), quant-ph/9511026.

[33] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca, Proc. Roy. Soc. London Ser. A **454**, 339 (1998), eprint quant-ph/9708016.

[34] D.S. Abrams and S. Lloyd, Phys. Rev. Lett. **83**, 5162 (1999).

[35] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2000).

[36] Joseph Emerson, Yaakov S. Weinstein, Marcos Saraceno, Seth Lloyd and David G. Cory, Science **302** (2003).

[37] M. Mohseni and D.A. Lidar, Phys. Rev. Lett. **97**, 170501 (2006).

[38] A. Ashikhmin, A. Barg, E. Knill, S. Litsyn (1999), quant-ph/9906126.

[39] A. Ashikhmin, A. Barg, E. Knill, S. Litsyn (1999), quant-ph/9906131.

[40] S. L. Braunstein, Phys. Rev. A **49**, 49 (1994).

[41] V. Giovannetti, S. Lloyd and L. Maccone, Science **306** (2004).

[42] K.R. Brown, R.J. Clark and I.L. Chuang, Phys. Rev. Lett. **97**, 050504 (2006).

[43] P. Jordan and E. Wigner, Z. Phys. **47** (1928).

[44] L.-A. Wu and D. A. Lidar, J. Math. Phys. **43**, 4506 (2002).

[45] G. Mahler and V.A. Weberruss, *Quantum Networks: Dynamics of Open Nanostructures* (Springer Verlag, Berlin, 1998), 2nd ed.

[46] M.S. Byrd and N. Khaneja, Phys. Rev. A **68**, 062322 (2003), ePrint `quant-ph/0302024`.

[47] Gen Kimura, Phys. Lett. A **314**, 339 (2003).